A HASSE PRINCIPLE FOR PERIODIC POINTS

ADAM TOWSLEY

ABSTRACT. Let F be a global field, let $\varphi \in F(x)$ be a rational map of degree at least 2, and let $\alpha \in F$. We say that α is periodic if $\varphi^n(\alpha) = \alpha$ for some $n \geq 1$. A Hasse principle is the idea, or hope, that a phenomenon which happens everywhere locally should happen globally as well. The principle is well known to be true in some situations and false in others. We show that a Hasse principle holds for periodic points, and further show that it is sufficient to know that α is periodic on residue fields for every prime in a set of natural density density 1 to know that α is periodic in F.

1. Introduction

We will call F a **global field** if F is a number field or if F is a function field with a finite field of constants. For a global field F let $\varphi : \mathbb{P}^1_F \to \mathbb{P}^1_F$ be a rational map. For any integer $n \geq 0$, write $\varphi^n(x) = \varphi \circ \varphi \circ \cdots \circ \varphi(x)$ for the nth iterate of $\varphi(x)$ under composition. The *forward orbit* of a point $\alpha \in F$ is defined to be $\mathcal{O}_\varphi(\alpha) = \{\alpha, \varphi(\alpha), \varphi^2(\alpha), \ldots, \}$. Similarly the *strict forward orbit* of α is defined to be $\mathcal{O}^+_\varphi(\alpha) = \{\varphi(\alpha), \varphi^2(\alpha), \ldots, \}$ and the *back orbit* of α is defined to be the set $\mathcal{O}^-_\varphi(\alpha) = \left\{\beta \in \mathbb{P}^1_{\overline{F}} : \varphi^n(\beta) = \alpha \text{ for some } n \geq 1\right\}$. A point α is said to be *periodic* if $\varphi^n(\alpha) = \alpha$ for some n, and more generally α is said to be *preperiodic* if its forward orbit is finite. If α has an infinite forward orbit we say that α is a *wandering point*. If the back orbit of α is finite then we say that α is an *exceptional point*.

For a prime ideal $\mathfrak{p} \subseteq F$ there is a well defined 'reduction mod $\mathfrak{p}$' map $r_\mathfrak{p} : \mathbb{P}^1_F \to \mathbb{P}^1_{F_\mathfrak{p}}$ where $F_\mathfrak{p}$ is the residue field of $\mathfrak{p}$. For any $\alpha \in F$ denote $r_\mathfrak{p}(\alpha)$ by $\overline{\alpha} \in F_\mathfrak{p}$. Similarly for any $\varphi \in F(x)$ denote by $\overline{\varphi}$ the reduction of φ modulo $\mathfrak{p}$, for all but finitely many primes $\overline{\varphi} : \mathbb{P}^1_{F_\mathfrak{p}} \to \mathbb{P}^1_{F_\mathfrak{p}}$ is a morphism. As $F_\mathfrak{p}$ is a finite field any $\overline{\alpha} \in F_\mathfrak{p}$ must be either periodic or strictly preperiodic. If $\overline{\alpha} \in F_\mathfrak{p}$ is periodic we will say that α has *periodic reduction* at $\mathfrak{p}$. Note that we could also define the reduced orbit of α modulo $\mathfrak{p}$ by taking the reduction of the ordered set of points $\mathcal{O}_\varphi(\alpha)$ modulo $\mathfrak{p}$. This definition corresponds to $\mathcal{O}_{\overline{\varphi}}(\overline{\alpha})$ if $\mathfrak{p}$ is a prime of good reduction for φ and is well defined if $\mathfrak{p}$ is a prime of bad reduction for φ. If $\mathfrak{p}$ is a prime of bad reduction for φ we will say α has periodic reduction at $\mathfrak{p}$ if its reduced orbit is periodic under the second definition.

Given any point $\alpha \in F$ one might ask if it is possible to determine if α is periodic in F based on its reduction modulo $\mathfrak{p}$ for various $\mathfrak{p}$? In other words, can local information about

Date: September 19, 2012.
2010 *Mathematics Subject Classification.* Primary 11S82, 37P05, 37P35.
Key words and phrases. Arithmetic Dynamics, Periodic Points, Integrality.

periodicity give global information? To that end we prove the following theorem which can be thought of as a Hasse principle for periodic points.

Theorem 1. *For a global field F, rational map $\varphi \in F(x)$ of degree at least 2, and point $\alpha \in F$ the following are equivalent:*

(i) *α is periodic.*
(ii) *α has periodic reduction for every prime $\mathfrak{p}$.*
(iii) *α has periodic reduction for every prime $\mathfrak{p} \in \mathcal{P}$, where $\mathcal{P}$ is a set of primes with natural density 1.*

Clearly $(i) \Rightarrow (ii) \Rightarrow (iii)$ so the only work involved is proving $(iii) \Rightarrow (i)$. To do this for number fields we use the following theorem of Benedetto, Ghioca, Hutz, Kurlberg, Scanlon, and Tucker from [1].

Theorem 1.1 (Benedetto, Ghioca, Hutz, Kurlberg, Scanlon, and Tucker)**.** *If F is a number field, $\varphi \in F(x)$ a rational map of degree at least 2, and $\alpha, \beta \in F$ are points such that $\beta \notin \mathcal{O}_{\varphi}^{+}(\alpha)$ then there is a set of primes $\mathcal{P}$ with positive density such that $\overline{\beta} \notin \mathcal{O}_{\overline{\varphi}}^{+}(\overline{\alpha})$ for every $\mathfrak{p} \in \mathcal{P}$.*

To complete the proof of Theorem 1 when F is a function field with a finite field of constants we prove Theorem 3, the analog of Theorem 1.1. A key element of Theorem 1.1 is that if α wanders then it will have non-periodic reduction for infinitely many primes. For a number field F this follows easily from the following theorem of Silverman which appears in [12].

Theorem 1.2 (Silverman)**.** *If F is a number field, $\varphi(x) \in F(x)$ is a rational map of degree at least 2, and $\alpha, \beta \in F$ are points such that β is not exceptional then only finitely many elements of $\mathcal{O}_{\varphi}(\alpha)$ are S-integral to β.*

We cannot use Silverman's Theorem when F is a function field with a finite field of constants since the proof requires Roth's Theorem, which is false for fields with positive characteristic (see section 6.2 in [4]). Thus we prove the following similar theorem.

Theorem 2. *If F is a global field, $\varphi \in F(x)$ is a rational map of degree at least 2, and $\alpha, \beta \in \mathbb{P}^1(F)$ are points such that β is periodic and not exceptional then only finitely many elements of $\mathcal{O}_{\varphi}(\alpha)$ are S-integral to β.*

As a corollary to Theorem 2 we are able to prove that if $\alpha \in F$ is not periodic then there are infinitely many primes $\mathfrak{p}$ for which α has non-periodic reduction. To prove Theorem 2 we will first prove Lemma 3.2 using Runge's method. Runge developed the method in the 1880's in [10]. In 1983, almost 100 years later, it was generalized by Bombieri in [3]. More recently Runge's method has been used by Levin in [9] and in a dynamical setting

by Corvaja, Sookdeo, Tucker, and Zannier in [5]. We will then apply Theorem 2 to recover several necessary dynamical results.

In Section 2 we give a definition of global fields and describe the important Northcott property, we also develop the notion of integrality. In Section 3 we prove a finiteness lemma which we apply to a dynamical setting in order to prove Theorem 2. In Section 4 we then apply Theorem 2 to prove Theorem 3 which is the function field analog of Theorem 1.1. Finally, in Section 6 we use Theorems 1.1 and 3 to prove the Hasse principle for periodic points, Theorem 1. Having proved Theorem 1 we discuss the possibility of strengthening it and the necessary conditions which would need to be applied.

Acknowledgments: The author would like to thank Tom Tucker and Xander Faber for their help preparing this paper.

2. Preliminaries

We now develop some of the necessary preliminary materials for proving Theorem. 2

2.1. **Global Fields and the Northcott Property.**

In the introduction we made the following definition.

Definition 2.1. *If F is either a number field or a function field with a finite field of constants then we say that F is a **global field**.*

These types of fields are distinguished for two reasons; they have finite residue fields and they have the Northcott property which we state here as a theorem.

Theorem 2.2 (The Northcott Property)**.** *If F is a global field, and N is any positive real number then there are only finitely many $\alpha \in F$ such that $h(\alpha) < N$.*

Proof. If F is a number field this is well known, for example see [13]. If F is a function field with a finite field of constants then the Northcott property follows from the fact that there are only finitely many elements $\alpha \in F$ of bounded degree. □

2.2. (a, S)**-Integers.**

Let F be a global field, one way of describing the ring of integers of F is the set $R = \{x \in F | r_{\mathfrak{p}}(x) \neq \infty$ for every prime $\mathfrak{p}\}$, in other words the set of all $x \in F$ with no 'denominator'. A standard generalization of R is to allow finitely many denominators. If S is a finite set of primes then the ring of S-integers is the set $R_S = \{x \in F | r_{\mathfrak{p}}(x) \neq \infty$ for every prime $\mathfrak{p} \notin S\}$. The rings of integers and S-integers are defined relative to ∞ and can be generalized further by replacing ∞ with an arbitrary point $a \in F$, and in fact by an entire set of points D. We thus make the following definition.

Definition 2.3. *If F is a global field, S is a finite set of places (containing the archimidean places) and D is a divisor then the (D, S)-integers are defined to be the set*

$$\{b \in F | f_{\mathfrak{p}}(b) \not\equiv 0 \mod \mathfrak{p} \textit{ for every } \mathfrak{p} \notin S\},$$

Where $f_{\mathfrak{p}}$ is a homogeneous polynomial defining D modulo $\mathfrak{p}$.

In other words b is a (D,S)-integer if b avoids D for all primes outside of S. If b is a (a,S)-integer then we say that b is S-integral to a. It is quick to see that the integrality relation is symmetric, that is b is S-integral to a if and only if a is S-integral to b. For far more details on integrality see Section 12 in [14].

3. Integrality

3.1. **Runge's Method.** In this section we will prove a finiteness result which is critical to Theorem 2. To begin we prove the following bound.

Proposition 3.1. *Let F be a global field, S be a finite set of places, and $f_1,\dots,f_t \in F[x]$ be distinct irreducible polynomials with leading coefficients $a_1,\dots,a_t$. Let $v \in S$ and let $C_v = \left[\frac{1}{2}\right]^d \cdot \left[\prod_i \min\{|a_i|_v, 1\}\right] \cdot \left[\prod \min\{|\beta-\gamma|_v, 1\}\right]$ where β and γ are taken to range over roots of all pairs polynomials $f_i \neq f_j$ and d is the maximal degree of the f_j. If $\alpha \in F$ then for all but at most one f_i we have that $|f_j(\alpha)|_v \geq C_v$.*

Proof. For any $v \in S$ fix an embedding $F \hookrightarrow \mathbb{C}_v$. Pick a root β_i of some f_i such that $|\alpha-\beta_i|_v \leq |\alpha-\beta|_v$ for each root β of of any f_j. For any $j \neq i$ we have that

$$\begin{aligned} |f_j(\alpha)|_v &= |a_j|_v \cdot \prod_{f_j(\gamma)=0} |\alpha-\gamma|_v \\ &\geq |a_j|_v \cdot \prod_{f_j(\gamma)=0} \frac{1}{2}|\beta_i-\gamma|_v \quad (\text{ since } |\alpha-\beta_i|_v \text{ is minimal}) \\ &\geq \left[\frac{1}{2}\right]^d \cdot \left[\prod_i \min\{|a_i|_v, 1\}\right] \cdot \left[\prod \min\{|\beta-\gamma|_v, 1\}\right] \\ &= C_v. \end{aligned}$$

We now use Proposition 3.1 to show that if a rational function has enough irreducible factors in relation to a set of primes S, then only finitely many points can be S-integral to its vanishing divisor.

Lemma 3.2. *Let F be a global field, and S be a finite set of places (containing the infinite places) with $|S| = r$. If $\varphi \in F(x)$ is a rational map where the numerator factors into irreducible polynomials $f_1,\dots,f_t$ with $t > r$ and D is the vanishing divisor of φ then there are at most finitely many points $\alpha \in F$ which are S-integral to D.*

Proof. By Proposition 3.1, for each $v \in S$ there is an effectively computable C_v such that for any γ we have that $|f_i|_v(\gamma) \geq C_v$ for all but at most one f_i. Since there are fewer places

$v\in S$ than there are polynomials f_i it follows that there is an f_k such that $|f_k(\gamma)|\geq C_v$ for every $v\in S$.

If γ is S-integral to D then applying the product formula it follows that

$$h(f_k(\gamma))=\sum_{v\in S}-n_v\log^-|f_k(\gamma)|_v\leq\sum_{v\in S}n_v\log C_v.$$

Where n_v is the local degree of v. Since $h(f_k(\gamma))\geq d_k h(\gamma)+M_k$, where $d_k=\deg(f_k)$ and M_k is an effectively computable constant which depends only upon f_k and not on γ, it follows that there is an effectively computable C such that

$$h(\gamma)\leq C.$$

Thus the set of such γ must be finite by Northcott.

3.2. **Integrality in Dynamics.** We are now prepared to prove Theorem 2.

Proof of Theorem 2. If α is preperiodic then $\mathcal{O}_\varphi(\alpha)$ is finite and the result is trivial. So assume that α wanders.

Let S be a finite set of primes which includes the archimidean primes and the primes of bad reduction. Additionally, let β have period k. As β is not exceptional, there exists an element $\beta_1\in\varphi^{-k}(\beta)\subseteq\overline{F}$ which is not in the periodic cycle of β. Thus the numerator of $\varphi^k(x)-\beta$ contains an irreducible polynomial factor, $g_1\in F[x]$, of which β_1 is a root. Similarly there is a $\beta_2\in\varphi^{-k}(\beta_1)$ which does not lie in the periodic cycle of β. As before we see that the numerator of $\varphi^{2k}(x)-\beta$ must contain an irreducible polynomial factor, $g_2\in F[x]$, of which β_2 is a root. Note that β_2 is not a root of g_1 and that β_1 is not a root of g_2. Proceeding inductively we are able to produce distinct irreducible polynomials $g_1,\dots,g_{r+1}\in F[x]$ where each g_i divides the numerator of $\varphi^{ik}(x)-\beta$. As β is periodic with period k it follows that all of the g_i are factors of the numerator of $\varphi^{k(r+1)}(x)-\beta$. We thus have a rational function, $\varphi^{k(r+1)}(x)-\beta\in F(x)$, where $r+1$ distinct irreducible polynomials divide the numerator.

Let D be the vanishing divisor of $\varphi^{k(r+1)}(x)-\beta$, note that since β is a root of $\varphi^{k(r+1)}(x)-\beta$ it is an element of D. Lemma 3.2 shows that there are only finitely many elements $\alpha\in F$ which are S-integral to D. Since $\varphi^n(\alpha)$ is S-integral to β if and only if $\varphi^{n-r-1}(\alpha)$ is S-integral to D it follows that there can be only finitely elements of $\mathcal{O}_\varphi(\alpha)$ which are S-integral to β. $\square$

Using the same notation we deduce the following corollaries.

Corollary 3.3. *If $\alpha\in F$ is a wandering point and $\beta\in F$ is a non-exceptional periodic point then there exists infinitely many prime ideals $\mathfrak{p}$ such that $\varphi^n(\alpha)\equiv\beta\mod\mathfrak{p}$ for some n.*

Proof. This is immediate from the definition of S-integrality. Since only finitely many elements of $\mathcal{O}_\varphi(\alpha)$ are S-integral to β for any finite set of primes S it follows that there must be infinitely many primes $\mathfrak{p}$ for which $\varphi^n(\alpha) \equiv \beta \mod \mathfrak{p}$ for some n. $\square$

Corollary 3.4. *Let $\varphi(x) \in F(x)$, and $\alpha \in F$ be non-periodic. There exists infinitely many primes $\mathfrak{p}$ for which α is not periodic modulo $\mathfrak{p}$.*

Proof. If α is preperiodic then its strict forward orbit $\mathcal{O}_\varphi^+(\alpha)$ is finite, denote it as $\{\alpha_1, \ldots, \alpha_l\}$. For any $1 \leq i \leq l$ only finitely many primes contain $(\alpha - \alpha_i)$, since there are only finitely many i we see that α can only have periodic reduction for finitely many primes.

Assume now that α wanders, after possibly passing to an extension E/F we can find a periodic $\beta_1 \in E$ which is not exceptional. Let β_1 have exact period k and let $\mathcal{O}_\varphi(\beta_1) = \{\beta_1, \beta_2, \ldots, \beta_k\}$. By Corollary 3.3 there are infinitely many primes $\mathfrak{p} \subseteq E$ such that $\varphi^n(\alpha) \equiv \beta_1 \mod \mathfrak{p}$. For each β_i there are only finitely many prime ideals which contain $(\alpha - \beta_i)$, so there are only finitely many primes for which $\alpha \equiv \beta_i \mod \mathfrak{p}$. Thus there are only finitely many primes for which α is in the periodic cycle of β_1 modulo $\mathfrak{p}$ and is thus periodic modulo $\mathfrak{p}$. Since there are infinitely many prime for which $\varphi^n(\alpha) \equiv \beta_1 \mod \mathfrak{p}$ for some n we have that $n > k$ infinitely often and therefore α must be strictly preperiodic infinitely often. $\square$

4. Intersections in Orbits

We will now prove the following analog to Theorem 1.1.

Theorem 3. *If F is a function field with a finite field of constants, $\varphi(x) \in F(x)$ a rational map with separability degree of at least 2, and $\alpha, \beta \in F$ are points such that $\beta \notin \mathcal{O}_\varphi^+(\alpha)$, then there is a set of primes $\mathcal{P}$ with positive natural density such that $\overline{\beta} \notin \mathcal{O}_{\overline{\varphi}}^+(\overline{\alpha})$ for any prime $\mathfrak{p} \in \mathcal{P}$.*

4.1. Separability, Ramification, and Density.

If F is a function field with a finite field of constants then F has positive characteristic. To begin proving Theorem 3 we must first account for the fact that not all finite extensions L/F are separable. Once these issues are dealt with we use Corollary 3.4 and reproduce the proof from [1]. We begin by making the following definitions.

Definition 4.1. *Let F be a function field with a finite field of constants, $\varphi \in F(x)$, $\varphi = \frac{f(x)}{g(x)}$, and $\deg(\varphi) = \max\{\deg(f), \deg(g)\} \geq 2$. We say that φ is* ***separable*** *(resp. inseparable, purely inseparable) if it induces a separable (resp. inseparable, purely inseparable) field extension.*

In addition to a rational function being separable we will require that it have separable reduction. A map $\varphi \in F(x)$ has **separable reduction** at a prime $\mathfrak{p}$ if the reduction of φ modulo $\mathfrak{p}$ is separable. We now show that having separable reduction is not a strong condition to impose.

Proposition 4.2. *If $\varphi \in F(x)$ is separable with degree at least 2, then φ has separable reduction for all but finitely many primes $\mathfrak{p}$ of F.*

Proof. Let F have characteristic p and write $\varphi = f/g$ for two relatively prime polynomials $f, g \in F[x]$. Since φ is separable there exists a term ax^l of either f or g for which $a \neq 0$ and $p \nmid l$. Let S be the set of primes of F which divide the numerator or denominator of $a \cdot \mathrm{Res}(\varphi)$. Then φ has separable good reduction for every $\mathfrak{p} \notin S$. □

If $\varphi \in F(x)$ is an inseparable rational function then it can be written as $\varphi(x) = h(x^r)$ where h is separable and r is the inseparable degree of φ. Let E/F be the splitting field of φ and define E^{sep} to be the maximal separable sub-extension, that is $F \subseteq E^{\mathrm{sep}} \subseteq E$. If $r \geq 2$ then E/E^{sep} is a purely inseparable extension so any prime $\mathfrak{p}$ of F will ramify in E. Because of this fact we will modify our definition of a ramified prime.

Definition 4.3. *For E and E^{sep} as above we say that a prime $\mathfrak{p}$ of F ramifies in E if it is ramified in E^{sep}.*

Recall that the **natural density** of a set of places S of a global field F is defined to be $D(S) = \lim\limits_{N\to\infty} \dfrac{\#\{\text{places } v \in S | N_v \leq N\}}{\#\{\text{places } v \in F | N_v \leq N\}}$, where NS_v is the size of the residue field of v. We will prove our density result for an extension L/F, however when sets of primes with positive density in a field L are intersected with a subfield F they will yield a set of primes with positive density in the subfield, though the density may decrease. We prove this fact now.

Lemma 4.4. *Let E be be a finite extension of any global field F with $[E:F] = d$. Let S_E be a set of primes of E with positive density δ and let $S_F = \{\mathfrak{p} = \mathfrak{q} \bigcap F | \mathfrak{q} \in S_E\}$. S_F has positive density γ where $\gamma \geq \frac{\delta}{d} > 0$.*

Proof. For each prime $\mathfrak{p}$ of F there are at most d primes $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_n$ of E such that $q_i \bigcap F = \mathfrak{p}$. Given any N, for every d primes $v \in S_E$ with $N_v \leq N$ there is at least one prime $\mathfrak{p} \in S_F$ with $N_p \leq N$. Taking the limit as $N \to \infty$ we see that the density of S_F is at least $\frac{\delta}{d} > 0$. □

To obtain our density result we adapt the arguments of [1] to prove lemmas 4.7, 4.8, and 4.9 in the function field setting. We will use Chebotarev's Density Theorem for function fields as proved by Murty and Scherk in [8] which states the following.

Theorem 4.5 (Chebotarev's Density Theorem for Function Fields)**.** *Let F be a function field with a finite field of constants, and E/F be a Galois extension with Galois group G. If $C \subset G$ is a conjugacy class, ψ is the number of unramified primes of E, ψ_C is the number of unramified primes of E whose Frobenius substitution corresponds to C then*

$$\left|\psi_C - \psi\frac{|C|}{|G|}\right| \leq \frac{B}{\sqrt{N}},$$

where N is the size of the constant field of F, and B is a constant depending on the genus of the curve associated to E, the ramification of E/F, $|C|$, and $|G|$.

4.2. **Proof of Theorem 3.** To use Theorem 4.5 it is necessary to have an unramified field extension, thus we prove the following lemmas relating critical points of φ to ramified primes in a field extension of F in the sense of Definition 4.3.

Lemma 4.6. *Let k be a complete and algebraically closed non-Archimidean field with non-trivial valuation, also let $\varphi \in k(x)$ be a rational function of degree at least 2 with good and separable reduction. If $\beta \in \mathbb{P}^1(k)$ is such that the reduction $\overline{\varphi}$ has a critical point at $\overline{\beta}$, then there is a critical point for φ lying in the same residue disk as β.*

Proof. By changing coordinates we may assume that $|\beta| \leq 1$ and that $|\gamma| \leq 1$ for every critical point γ of φ. Writing $\varphi = f/g$ for relatively prime polynomials $f, g \in \mathfrak{o}_k[x]$. The roots of the Wronskian of φ are precisely the critical points of φ and

$$\mathrm{Wr}_{\varphi}(x) = g(x) f'(x) - g'(x) f(x) = a \prod_{\varphi'(\gamma)=0} (x - \gamma),$$

for some $a \in \mathfrak{o}_k$. Since φ has good separable reduction, the reduction of the last expression is not identically zero and in particular $|a| = 1$. Evaluating the reduction at $\overline{\beta}$ shows that

$$0 = \mathrm{Wr}_{\overline{\varphi}}(\overline{\beta}) = \overline{\mathrm{Wr}(\beta)} = \overline{a} \prod_{\varphi'(\gamma)=0} (\overline{\beta} - \overline{\gamma}).$$

It follows that $\overline{\beta} = \overline{\gamma}$ for some critical point γ, proving the lemma. □

We now apply this local result to our global field F.

Lemma 4.7. *Let $\tilde{\mathfrak{p}}$ be a prime of $\mathfrak{o}_{\overline{F}}$ (where $\overline{F}$ is an algebraic closure of F and $\mathfrak{o}_{\overline{F}}$ is its ring of integers), and let $\varphi = h(x^r) \in F(x)$ be a rational map of separable degree $d \geq 2$, where h is separable and r is the inseparable degree of φ. Let $\mathfrak{p} = \tilde{\mathfrak{p}} \bigcap \mathfrak{o}_F$ be a prime such that h has good and separable reduction at $\mathfrak{p}$. Also let $\alpha \in \mathbb{P}^1(F)$, E the splitting field of $\varphi(x) - \alpha$, $\beta \in \varphi^{-1}(\alpha) \subseteq \mathbb{P}^1(E)$, and $\mathfrak{p}' := \tilde{\mathfrak{p}} \bigcap E$. If $\mathfrak{p}'$ is ramified over $\mathfrak{p}$ then β is congruent modulo $\tilde{\mathfrak{p}}$ to a ramification point of φ^m.*

Proof. Let $|\cdot|_{\tilde{\mathfrak{p}}}$ be the $\tilde{\mathfrak{p}}$-adic absolute value on $\overline{F}$. By changing coordinates we can assume that $\alpha = 0$ and $|\beta|_{\tilde{\mathfrak{p}}} \leq 1$. Let $h(x) = \frac{f(x)}{g(x)}$ ($f, g \in F[x]$). As $\varphi(\beta) = \alpha = 0$ we have that $h(\beta) = f(\beta) = 0$. Since $\mathfrak{p}'$ is ramified over $\mathfrak{p}$, by definition $\mathfrak{p}$ is ramified in E^{sep}, the maximal separable sub-extension of E. Additionally, since $\mathfrak{p}'$ is ramified f must have at least one other root congruent to β modulo $\tilde{\mathfrak{p}}$, thus $\overline{f}$ has a multiple root at β. Since h has good reduction at $\mathfrak{p}$, $\overline{g}(\beta) \neq 0$, therefore $\overline{h}$ has a multiple root at β, hence $\overline{h}'(\beta) = 0$. Applying Lemma 4.6 finishes the proof. □

Using Lemma 4.7 we now show that there there is a field extension L/F where we can find an unramified extension with the necessary extension of residue fields.

Lemma 4.8. *Let $\tilde{\mathfrak{p}}$ be a prime of $\mathfrak{o}_{\overline{F}}$ and let $\varphi \in F(x)$ be a rational function with separable degree $d \geq 2$, and separable good reduction at $\mathfrak{p} = \tilde{\mathfrak{p}} \bigcap \mathfrak{o}_F$, and let $\beta \in \mathbb{P}^1(F)$. Then there exists a finite extension E of F with the following property: for any finite extension L of E, there is a positive integer M such that for any $m \geq M$ and all $\alpha \in \mathbb{P}^1\left(\overline{F}\right)$ with $\varphi^m(\alpha) = \beta$,*

(i) *τ does not ramify over $\mathfrak{p}'$, and*
(ii) $\left[\mathfrak{o}_{L(\alpha)}/\tau : \mathfrak{o}_L/\mathfrak{p}'\right] > 1$

where $\tau := \tilde{\mathfrak{p}} \bigcap \mathfrak{o}_{L(\alpha)}$ and $\mathfrak{p}' = \tilde{\mathfrak{p}} \bigcap \mathfrak{o}_L$.

Proof. We begin by assuming that β is not periodic modulo $\mathfrak{p}$. In this case for any $\gamma \in \mathfrak{o}_{\overline{F}}$, there is at most one $j \geq 0$ such that

$$\varphi^j(\gamma) \equiv \beta \mod \tilde{\mathfrak{p}}. \tag{4.1}$$

In particular, for each ramification point $\gamma \in \mathbb{P}^1\left(\overline{F}\right)$ of φ, there are only finitely many integers $n \geq 0$ and points $z \in \mathbb{P}^1\left(\overline{F}\right)$ such that $\varphi^n(z) = \beta$ and $z \equiv \gamma \mod \tilde{\mathfrak{p}}$. Let E be the finite extension of F formed by adjoining all such points z.

Given any finite extension L of E, let $\mathfrak{p}' = \tilde{\mathfrak{p}} \bigcap \mathfrak{o}_L$. Since $\mathbb{P}^1(\mathfrak{o}_L/\mathfrak{p}')$ is finite, (4.1) implies that for all sufficiently large M, $\varphi^M(x) = \beta$ has no solutions in $\mathbb{P}^1(\mathfrak{o}_L/\mathfrak{p}')$. Fix any such M; note that M must be larger than any of the integers n above. Hence, given any $m \geq M$ and $\alpha \in \mathbb{P}^1\left(\overline{F}\right)$ such that $\varphi^m(\alpha) = \beta$, we must have $\left[\mathfrak{o}_{L(\alpha)}/\tau : \mathfrak{o}_L/\mathfrak{p}'\right] > 1$, where $\tau = \tilde{\mathfrak{p}} \bigcap \mathfrak{o}_{L(\alpha)}$, proving (ii). Furthermore, if α is a root of $\varphi^m(x) - \beta$, then there are two possibilities: either (1) α is not congruent modulo $\tilde{\mathfrak{p}}$ to a ramification point of φ^m, or (2) $\varphi^j(\alpha) = z$ for some $j \geq 0$ and some point $z \in \mathbb{P}^1(L)$ from the previous paragraph. In case (1), τ is unramified over $\mathfrak{p}'$ by Lemma 4.7. In case (2), choosing a minimal such $j \geq 0$, and applying Lemma 4.7 with z in the roll of β and j in the role of m, τ is again unramified over $\mathfrak{p}'$. Thus (ii) holds.

If β is periodic modulo $\mathfrak{p}$ we will assume that it is fixed and then apply the above prove to each of the $\gamma_i \in \varphi^{-1}(\beta) \setminus \{\beta\}$ and produce a field E_i with the stated properties. To do this we note that no γ_i is periodic modulo $\tilde{\mathfrak{p}}$ as $\gamma_i \not\equiv \beta \mod \tilde{\mathfrak{p}}$; otherwise the ramification index of φ at β would be greater modulo $\tilde{\mathfrak{p}}$ than over F which contradicts the hypothesis of good and separable reduction. As $\gamma_i \not\equiv \beta \mod \tilde{\mathfrak{p}}$ it must be strictly preperiodic.

For each E_i let M_i be the constant as defined above, let $M = \max_i(M_i) + 1$ and let E be the compositum of the E_i. For any $m \geq M$ and $\alpha \in \mathbb{P}^1\left(\overline{F}\right)$ such that $\varphi^m(\alpha) = \beta$ but $\varphi^t(\alpha) \neq \beta$ for any $0 \leq t < m$ it follows that $\varphi^{m-1}(\beta) \neq \alpha$. Thus $\varphi^{m-1}(\beta)$ is one of the non periodic γ_i. Applying the arguments above for the γ_i we see that β satisfies conditions (i) and (ii). $\square$

We now have enough tools to prove Theorem 3. We begin by showing the result holds when α is not periodic.

Lemma 4.9. *Let F be a function field with a finite field of constants. If $\varphi \in F(x)$ and $\alpha, \beta \in F$, where φ is a rational function with separable of degree at least 2, α is not periodic and $\beta \notin \mathcal{O}_{\varphi}^{+}(\alpha)$, then there is a set of primes $\mathcal{P}$ of positive density such that for any $\mathfrak{p} \in \mathcal{P}$ and $n \geq 1$ we have*

$$\varphi^{n}(\alpha) \not\equiv \beta \mod \mathfrak{p}.$$

Proof. By Corollary 3.4 there are infinitely many primes $\mathfrak{p}$ of F for which α has non-periodic reduction. As there are only finitely many primes of bad reduction and finitely many primes with inseparable reduction we can choose a prime τ of F of good reduction for which α is not periodic.

By Lemma 4.8 there is a finite extension E/F which satisfies the conclusions of the lemma. E can be thought of as a finite extension of itself. By Lemma 4.4 it suffices to prove the result for E. Let $\mathfrak{p}$ be a prime of E extending τ. For a sufficiently large integer M, and each $w \in \overline{F}$ such that $\varphi^{m}(w) = \beta$ but $\varphi^{t}(w) \neq \beta$ for every $0 \leq t < M$ we have

(i) $\mathfrak{p}'$ does not ramify over $\mathfrak{p}$, and
(ii) $\left[\mathfrak{o}_{E(w)}/\mathfrak{p}' : \mathfrak{o}_{E}/\mathfrak{p}\right] > 1$.

Where $\mathfrak{p}'$ is a prime of $E(w)$ extending $\mathfrak{p}$.

Fix such an M, and let L/E be the splitting field for φ^{M}, and note that this is a Galois extension as it is a splitting field. Also, by property (i) above L/E is unramified over $\mathfrak{p}$. By property (ii), the Frobenius element of $\mathfrak{p}$ belongs to a conjugacy glass of $G := \mathrm{Gal}(L/E)$ whose members do not fix any of the point w. By the Chebotarev Density Theorem, 4.5, this implies that there is a set of primes, $\mathcal{P}$, with positive density whose Frobenius conjugacy class in $\mathrm{Gal}(L/F)$ fix none of the w.

Fix any prime $\pi \in \mathcal{P}$. Let $m \geq 0$ be an integer and $z \in E$ be a point such that $\varphi^{m}(z) \equiv \beta \mod \pi$. We claim that there is some $0 \leq n < M$ such that $\varphi^{n}(z) \equiv \beta \mod \pi$.

To begin the proof note that if $m < M$ we are already done, so assume that $m \geq M$. We can also assume that m is the minimal integer $m \geq M$ such that $\varphi^{m}(z) \equiv \beta \mod \tau$. By the definition of $\mathcal{P}$, there can be no $c \in E$ such that $\varphi^{M}(c) \equiv \beta \mod \pi$ where $\varphi^{t}(c) \not\equiv \beta \mod \pi$ for every $0 \leq t < M$.

Let $c = \varphi^{m-M}(z) \in E$. As m was chosen to be the minimal integer greater than M there must be a t, with $0 \leq t < M$, such that $\varphi^{t}\left(\varphi^{m-M}(z)\right) \equiv \beta \mod \pi$. So $\varphi^{m-M+t}(z) \equiv \beta \mod \pi$. But $0 \leq m - M + t < m$, which contradicts the minimality of m. Proving the claim.

If β is preperiodic (including the case where β is periodic), then let $\mathcal{U} \subseteq \mathcal{P}$ be the set of primes π such that $\varphi^{t}(\alpha) \equiv \beta \mod \pi$, for some $0 \leq t < M$. $\mathcal{U}$ is a finite set. Remove the primes of $\mathcal{U}$ from $\mathcal{P}$ and note that, as $\mathcal{U}$ is finite, the density of $\mathcal{P}$ has not changed.

If β is not preperiodic, then let $\mathcal{V} \subseteq \mathcal{P}$ be the set of primes π such that $\varphi^t(\beta) \equiv \beta \mod \pi$ for some $1 \leq t < M$. $\mathcal{V}$ is a finite set. Remove the primes of $\mathcal{V}$ from $\mathcal{P}$ and again note that, as $\mathcal{V}$ is finite, the density of $\mathcal{P}$ has not changed.

Suppose there is a $\pi \in \mathcal{P}$ and an integer $m \geq M$ such that $\varphi^m(\alpha) \equiv \beta \mod \pi$. Then by the earlier claim there is a $0 \leq t < M$ such that $\varphi^t(\alpha) \equiv b \mod \pi$. So by the construction of $\mathcal{U}$ we must have that β is not preperiodic. Since $\varphi^{m-t-1}(\varphi(\beta)) \equiv \beta \mod \pi$, and because $m - t - 1 \geq 0$, the claim tells us that there is a $0 \leq k < M$ such that $\varphi^{k+1}(\beta) \equiv \beta \mod \pi$. But this is impossible by the construction of $\mathcal{V}$. Proving the lemma. □

After applying Lemma 4.9 all that remains to prove of Theorem 3 is the case where α is periodic. We will now examine that case and conclude the proof.

Proof of Theorem 3. If α is not periodic then Theorem 3 follows from Lemma 4.9. If α is periodic then it has a finite orbit $\mathcal{O}_\varphi(\alpha) = \{\alpha = \alpha_0, \alpha_1, \ldots, a_m\}$. Since only finitely many primes contain the set of $\beta - a_i$ it follows that for any prime $\mathfrak{p}$ outside of that finite set $\varphi^n(\alpha) \not\equiv \beta \mod \mathfrak{p}$ for every n. □

4.3. **Stronger Non-Periodic Reduction.** We now apply Theorem 3 and Theorem 1.1 to prove a stronger version of Corollary 3.4. Recall that Corollary 3.4 says that if F is a global field, $\varphi \in F(x)$ is a rational function of degree at least 2, and $\alpha \in F$ wanders then there are infinitely many primes $\mathfrak{p}$ for which α has non-periodic reduction. Theorem 3 allows us to say something about the this infinite set of primes.

Corollary 4.10. *Let F be a global field, $\varphi \in F(x)$ a rational map of degree at least 2 and let $\alpha \in F$ be a non-periodic point. There exists a set of primes S with positive density such that α does not have periodic reduction for any prime $\mathfrak{p} \in S$.*

Proof. Since α is not periodic, by definition $\alpha \notin \mathcal{O}_\varphi^+(\alpha)$. Thus by Theorems 3 and 1.1 there is a set of primes $\mathcal{P}$ with positive density for which $\varphi^n(\alpha) \not\equiv \alpha \mod \mathfrak{p}$ for any $\mathfrak{p} \in \mathcal{P}$ and every $n \geq 1$. Thus α does not have periodic reduction for any $\mathfrak{p} \in S$. □

5. An Expansion Theorem 3

In this section we expand Theorem 3 in the style of [1] to include sets of points instead of a single α and β.

Theorem 4. *Let F be a function field with a finite field of constants and let $\varphi_1, \ldots, \varphi_g : \mathbb{P}^1(F) \to \mathbb{P}^1(F)$ be a set of rational maps each with separable degree at least 2. Let $\mathcal{A}_1, \ldots, \mathcal{A}_g$ be finite subsets of $\mathbb{P}^1(F)$ such that no $\mathcal{A}_i$ contain a φ_i-preperiodic point and let $\mathcal{B}_1, \ldots, \mathcal{B}_g$ be finite subsets of $\mathbb{P}^1_F$ such that at most one $\mathcal{B}_i$ contains a point which is not φ_i-preperiodic, and that there is at most one such point in that set. There is a set of primes $\mathcal{P}$ of F with*

positive density and a positive integer M such that for any $i = 1, \dots, g$, any $\alpha \in \mathcal{A}_i$, any $\beta \in \mathcal{B}_i$, any $\mathfrak{p} \in \mathcal{P}$, and every $n \geq M$,

$$\varphi^n(\alpha) \not\equiv \beta \mod \mathfrak{p}.$$

Remark 5.1. *Theorem 4 is both stronger and slightly weaker than Theorem 3. Theorem 4 is stronger because it allows for sets of points and it makes no requirement about the intersection of orbits in F. It is weaker because it does not allow any of the α to be preperiodic, as Theorem 3 does, and, since the wandering β may be in the orbit of an α, we are not able to remove the possiblity that $M > 0$.*

Proof. The proof of Theorem 3.1 in [1] works exactly for proving Theorem 4 if one replaces their use of Lemma 4.3 from [2] with Theorem 3.4 and replaces their Proposition 3.4 with Proposition 5.2 below. □

The following Proposition applies Lemma 4.8 to a set of points $\mathcal{B}$.

Proposition 5.2. *Let F be a function field with a finite field of constants, let $\tilde{\mathfrak{p}}$ be a prime of $\mathfrak{o}_{\overline{F}}$, and let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational function defined over F with separable degree at least 2 and with separable good reduction at $\mathfrak{p} = \tilde{\mathfrak{p}} \bigcap \mathfrak{o}_F$. Let $\mathcal{B} = \{\beta_1, \beta_2, \dots, \beta_n\} \subset \mathbb{P}^1(F)$ be such that for each $\beta_i \in \mathcal{B}$ either*

- *if β_i is not periodic, then β_i is not periodic modulo $\mathfrak{p}$; and*
- *if β_i is periodic, then $\varphi(\beta_i) = \beta_i$ and the ramification index of φ at β_i is the same modulo $\mathfrak{p}$ as over F.*

There exists a finite extension E of F with the following property: for any extension L of E, there is an integer $M \geq 0$ such that for all $m \geq M$ and all $\alpha \in \mathbb{P}^1(F)$ with $\varphi^m(\alpha) \in \mathcal{B}$ but $\varphi^t(\alpha) \notin \mathcal{B}$ for any $t < m$,

(1) *τ does not ramify over $\mathfrak{q}$, and*
(2) *$\left[\mathfrak{o}_{L(\alpha)}/\tau : \mathfrak{o}_L/\mathfrak{q}\right] > 1$,*

where $\tau := \tilde{\mathfrak{p}} \bigcap \mathfrak{o}_{L(\alpha)}$ and $\mathfrak{q} := \tilde{\mathfrak{p}} \bigcap \mathfrak{o}_L$.

Proof. The proof is the same as that of Proposition 3.4 in [1]. The requirement of separable degree of at least 2 for φ is in place so that we can apply Lemma 4.8 in place of their Lemma 3.3. □

6. A Hasse Principle for Periodic Points

We now complete the proof of Theorem 1.

Proof of Theorem 1. It is left to show that if $\alpha \in F$ has periodic reduction for every prime $\mathfrak{p} \in \mathcal{P}$ where $\mathcal{P}$ is a set of primes with positive natural density 1 then α is periodic in F. We will prove the contrapositive.

If α is not periodic then by Corollary 4.10 there is a set of primes S with positive density for which α has non-periodic reduction. Thus it is impossible for α to have periodic reduction on a set of primes $\mathcal{P}$ with density 1. $\square$

One might ask if the set $\mathcal{P}$ of primes with density 1 can be replaced by a set with a slightly smaller density? As stated the answer is no. Consider the family of polynomial maps $\varphi_q : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ given by $\varphi_q(x) = x^q + 1$, where $q \in \mathbb{Z}$ is an odd prime. Let $\mathcal{P}_q$ be the set of primes $\mathcal{P}_q = \{p \in \mathbb{Z} : p \not\equiv 1 \mod q\}$, and note that $\mathcal{P}_q$ has natural density $\frac{q-2}{q-1}$.

For any prime $p \in \mathcal{P}_q$ the residue field $\mathbb{F}_p$ does not contain a qth root of unity and therefore $\varphi_q(x) = x^q + 1$ is injective on the finite set $\mathbb{F}_p$. This means that $\overline{\varphi}_q(x)$ is a permutation of $\mathbb{F}_p$. When a permutation of a set is iterated every point is periodic, in particular $\alpha = 0$ is periodic under the map $\overline{\varphi_q}(x)$ for every prime $p \in \mathcal{P}_q$. In other words 0 has a periodic reduction for every prime $p \in \mathcal{P}_q$, but 0 is a wandering point of $\varphi_q(x)$ in $\mathbb{Q}$. Taking q to be sufficiently large we produce a set of primes, $\mathcal{P}_q$, with density arbitrarily close to 1 and a map $\varphi_q(x)$ for which $\alpha = 0$ wanders but has periodic reduction on $\mathcal{P}$.

We have demonstrated a wandering points with non-periodic reduction only on sets of arbitrarily small positive density, but we did it by using maps of very large degree. One could hope to recover a weaker statement by bounding the degree of the map $\varphi(x)$. So we are left with the following question.

Question 6.1. *For a global field F, and a rational map $\varphi \in F(x)$ of degree d, is there a constant C (depending on d) such that for any set of primes $\mathcal{P}$ with density D satisfying $1 - D < C$ the following holds: If $\alpha \in F$ has periodic reduction for every $\mathfrak{p} \in \mathcal{P}$ then must α be periodic in F?*

We conclude with a heuristic as why such a C should exist and propose a value. As usual let F be a global field, and $\varphi \in F(x)$ a rational map of degree $d \geq 2$. A wandering point $\alpha \in F$ will have periodic reduction on a set of primes $\mathcal{P}$ with a large density if that periodic reduction happens for some reason other than α being periodic, such as $\overline{\varphi}$ inducing a permutation on the residue field at every $\mathfrak{p} \in \mathcal{P}$. For a F is a number field recall that for any prime $\mathfrak{p}$ we denote by $F_{\mathfrak{p}}$ the residue field of $\mathfrak{p}$. If F is a number field then Schur made the following conjecture in [11]; if $\varphi(x) \in F[x]$ is a polynomial which is bijective on $F_{\mathfrak{p}}$ for infinitely many $\mathfrak{p}$ then either $\varphi(x) = ax^n + c$ or $\varphi(x) = T_n(x)$ (the n-th Chebychev polynomial). Fried proved Schur's conjecture in [6] and Guralnick, Müller, and Saxl generalized the result to rational functions in [7], however by allowing all rational maps the possible types of maps which induce a permutation on infinitely many $F_{\mathfrak{p}}$ must be

expanded. These results imply that maps of the form $\varphi(x) = x^d + c$ are in a sense 'worst-possible'. However for each map in this family there is only one 'bad' Chebotarev class of primes, the primes which are 1 modulo q. The density of these 'bad' primes is $\frac{1}{\phi(d)}$ where ϕ is the Euler ϕ-function. We therefore propose that $C = \frac{1}{\phi(d)}$ is the value which will give an affirmative answer to Question 6.1.

References

[1] Robert Benedetto, Dragos Ghioca, Benjamin Hutz, Pr Kurlberg, Thomas Scanlon, and Thomas Tucker. Periods of rational maps modulo primes. *Mathematische Annalen*, pages 1–24. 10.1007/s00208-012-0799-8. 1, 4.1, 4.1, 5, 5, 5

[2] Robert L. Benedetto, Dragos Ghioca, Pär Kurlberg, and Thomas J. Tucker. A case of the dynamical Mordell-Lang conjecture. *Math. Ann.*, 352(1):1–26, 2012. 5

[3] Enrico Bombieri. On Weil's "théorème de décomposition". *Amer. J. Math.*, 105(2):295–308, 1983. 1

[4] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006. 1

[5] C. Corvaja, V. Sookdeo, T. Tucker, and U. Zannier. Integral points in two-parameter orbits. *arXiv:1201.1313v2 [math.NT]*. 1

[6] Michael Fried. On a conjecture of Schur. *Michigan Math. J.*, 17:41–55, 1970. 6

[7] Robert M. Guralnick, Peter Müller, and Jan Saxl. The rational function analogue of a question of Schur and exceptionality of permutation representations. *Mem. Amer. Math. Soc.*, 162(773):viii+79, 2003. 6

[8] Vijaya Kumar Murty and John Scherk. Effective versions of the Chebotarev density theorem for function fields. *C. R. Acad. Sci. Paris Sér. I Math.*, 319(6):523–528, 1994. 4.1

[9] Aaron Levin. Variations on a theme of Runge: effective determination of integral points on certain varieties. *J. Théor. Nombres Bordeaux*, 20(2):385–417, 2008. 1

[10] Carl Runge. Uber das produkt funf aufeinander folgender zahlen in einer arithmetischen reihe. *J. Reine Angew. Math.*, 100:425–435, 1887. 1

[11] Issai Schur. Über den zusammenhang zwischen einem problem der zahlentheorie und einem satz ber algebraische funktionen. *S.-B. Preuss. Akad. Wiss. Berlin*, pages 123–134, 1923. 6

[12] Joseph H. Silverman. Integer points, Diophantine approximation, and iteration of rational maps. *Duke Math. J.*, 71(3):793–829, 1993. 1

[13] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007. 2.1

[14] Paul Vojta. Diophantine approximation and Nevanlinna theory. In *Arithmetic geometry*, volume 2009 of *Lecture Notes in Math.*, pages 111–224. Springer, Berlin, 2011. 2.2

Adam Towsley, Department of Mathematics, CUNY Graduate Center, 365 5th Avenue, New York, NY 10016-4309,

E-mail address: `atowsley@gc.cuny.edu`